

UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Information Associated with  
01bifftannen@gmail.com, jessicagilmore24hs@gmail.com  
ramonaenibarra@gmail.com, annebeason47@gmail.com  
ameliagrey24hs@gmail.com, pennysenn24hs@gmail.com  
that is stored at premises controlled by Google, Inc.

Case No. 16-M-1238

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 21, United States Code, Sections 829(e), 841(a)(1), 841(h), and 843(c)(2)(A)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached affidavit.



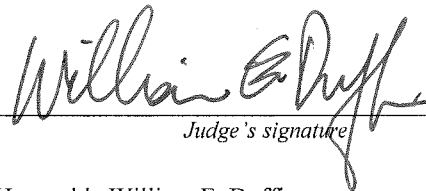
Applicant's signature

Scott Simons, Task Force Officer

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/31/16



Judge's signature

Honorable William E. Duffin

City and State: Milwaukee, Wisconsin

, U.S. Magistrate Judge

Printed Name and Title

**AFFIDAVIT IN SUPPORT OF  
APPLICATIONS FOR SEARCH WARRANTS**

I, Scott Simons, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications for search warrants for information associated with certain accounts that is stored at premises controlled by Google, Inc. ("Google") an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California and Yahoo! Inc. ("Yahoo"), an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google and Yahoo to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer assigned to the Milwaukee Office of the Drug Enforcement Administration (DEA) as a member of the Tactical Diversion Squad (TDS) specializing in pharmaceutical investigations. I have worked full-time as a Federal Task Force Officer for the past 3 years and a full-time law enforcement officer with the Greenfield Police Department for the past 14 years.

3. During my tenure as a DEA Task Force Officer and a Greenfield Police Department law enforcement officer, I have been involved in the investigation of narcotics traffickers operating not only in the County of Milwaukee and the State of Wisconsin but also other states throughout the United States. I have received training in the investigation of drug trafficking and computer related crimes. I have worked with informants in the investigations of drug trafficking in the Milwaukee area as well as other jurisdictions within the State of Wisconsin and throughout the United States. I have participated in the application for and execution of numerous search warrants. I have participated directly in numerous narcotics investigations and arrests in which controlled substances and drug paraphernalia were seized. I am familiar with methods that are commonly used by drug dealers to package and prepare controlled substances for sale in various areas.

4. Based on my training, experience, and participation in drug trafficking and computer related investigations, I know and have observed the following:

a. I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin as well as in other areas of the United States;

b. I am familiar with the coded language utilized over the telephone and other electronic communications to discuss drug trafficking and know that the language is often limited, guarded and coded. I also know the various code names used to describe controlled substances;

c. I know drug dealers often put telephones in the names of others (nominees) in order to distance themselves from telephones that they use to facilitate drug distribution. Because drug traffickers go through many telephone numbers, they often do not pay final bills when they are done using a telephone number and then are unable to put another line in the name of that subscriber;

d. I know drug traffickers often purchase and/or title assets in fictitious names, aliases or the names of relatives, associates or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;

e. I know drug traffickers must maintain on-hand large amounts of U.S. currency to include stored in financial accounts readily accessible in order to maintain and finance their ongoing drug business;

f. I know it is common for drug traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances. The aforementioned book, records, receipts, notes, ledger, etc., are maintained where the traffickers have ready access to them. These may be in paper form as well as in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;

g. I know it is common for large-scale drug traffickers to secrete contraband, proceeds of drug sales and records of drug transactions in secure locations within their residences, their businesses and/or other locations over which they maintain dominion and control, for ready access and to conceal these items from law enforcement authorities;

h. I know it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, passbooks, letters of credit, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control, as well as in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;

i. I know large-scale drug traffickers often use electronic equipment such as telephones (land-lines and cell phones), pagers, computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;

j. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency;

k. I know drug traffickers commonly maintain addresses or telephone numbers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization in papers and books as well as in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;

l. I know drug traffickers take or cause to be taken photographs or videos of themselves; their associates, their property and their drugs. These traffickers usually maintain these photographs or videos in their possession, often in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;

m. I am familiar with computers, cellular telephones, Smartphones, pagers and their uses by drug traffickers to communicate with suppliers, customers, and fellow traffickers; Drug traffickers use these devices to record their transactions and aspects of their lifestyle related to drug dealing, whether in the form of voicemail, email, text messages, video and audio clips, floppy disks, hard disk drives, thumbnail drives, CD's, DVD's, optical disks, Zip disks, flash memory cards, Smart media and any data contained within such computers or cellular telephones, electronic storage media and other settings particular to such devices; I know that such devices automatically record aspects of such communications, such as lists of calls and communications, and any particularized identification assigned to those source numbers or email addresses by the owner of the devices;

n. I know the following information can be retrieved to show evidence of use of a computer or Smartphone to further the drug trade: system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; computer media and any data contained within such media; operating system software, application or access program disks, manuals, books, brochures, or notes, computer access codes, user names, log files, configuration files, passwords, screen names, email addresses, IP addresses, and SIM cards.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 829(e) and 841(a)(1) (Distribution of Controlled Substances), and Title 21, United States Code, Sections 841(h) and 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet) have been committed by Anthony T. Hardy and others. There is also probable cause to search the locations described in Attachment A for fruits, evidence and instrumentalities of these crimes further described in Attachment B.

### **JURISDICTION**

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

### **STATUTORY BACKGROUND**

8. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 amended the Controlled Substances Act to address online pharmacies, codified at Title 21, United States Code (U.S.C.), § 829. No controlled substance that is a prescription drug as determined by the Federal Food, Drug and Cosmetic Act may be delivered, distributed, or dispensed by means of the Internet without a valid prescription, as



required by Title 21, Code of Federal Regulations (C.F.R.) § 1306.09(a) in violation of Title 21, U.S.C. § 829(e), § 841(a)(1) (Distribution of Controlled Substances) and 21 U.S.C. § 841(h), § 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet). According to Title 21 U.S.C. § 829, the term “valid prescription” means a prescription that is issued for a legitimate medical purpose in the usual course of professional practice by a practitioner who has conducted at least 1 in-person medical evaluation of the patient or a covering practitioner. The term “in-person medical evaluation” means a medical evaluation that is conducted with the patient in the physical presence of the practitioner, without regard to whether portions of the evaluation are conducted by other health professionals. The term “covering practitioner” means, with respect to the patient, a practitioner who conducts a medical evaluation (other than an in-person medical evaluation) at the request of a practitioner who has conducted at least 1 in-person medical evaluation of the patient or an evaluation of the patient through the practice of telemedicine, within the previous 24 months and is temporarily unavailable to conduct the evaluation of the patient.

9. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 also added new provisions to prevent the illegal distribution of controlled substances by means of the Internet including registration requirements of online pharmacies, Internet pharmacy website disclosure information requirements and prescription reporting requirements for online pharmacies. According to C.F.R. § 1301.11(b) as provided in § 303(f) and § 401(h) of the Act (21 U.S.C. § 823(f) and § 841(h)), it is unlawful for any person who falls within the definition of “online pharmacy” (as set forth in §102(52) of

the Act (21 U.S.C. § 802.52) and C.F.R. § 1300.4(h)) to deliver, distribute or dispense a controlled substance by means of the Internet if such person is not validly registered with a modification of such registration authorizing such activity (unless such person is exempt from such modified registration requirement under the Act or this chapter). A check of DEA records does not identify Goldpharma24 as a registered online pharmacy.

#### **PROBABLE CAUSE**

10. In February of 2015, the Milwaukee District Office of the DEA initiated an investigation into the internet pharmacy GOLDPHARMA24 located at [www.goldpharma-24.com](http://www.goldpharma-24.com), which advertises for sale controlled and non-controlled pharmaceuticals, including schedule II controlled substances, without requiring a prescription for such substances. Examination of public internet resources revealed that ANTHONY T. HARDY ("HARDY") was affiliated with the domain [www.goldpharma-24.com](http://www.goldpharma-24.com) and case agents' investigation identified HARDY as being affiliated with multiple pharmacy affiliate groups and thousands of pharmaceutical domains were registered by HARDY.

11. The customer service phone number listed on the GOLDPHARMA24 internet pharmacy website is (810) 487-4516, which is a telephone number provided by Nextiva phone company. Subpoenaed account information from Nextiva reveals that (810) 487-4516 was one of thirteen (13) telephone numbers assigned to this account. Case agents conducted internet searches of these thirteen (13) telephone numbers associated with GOLDPHARMA24's phone number and found dozens of other similar



internet pharmacies and potentially counterfeit product websites associated with these (13) telephone numbers.

12. Subpoenaed account information revealed that these telephone numbers, including GOLDPHARMA24's customer service phone number, listed to JESSICA GILMORE, with a billing email listed as **jessicagilmore24hs@gmail.com**, and RAMONA ENRIQUITA IBARRA was listed as the credit card billing name. Subpoenaed records revealed that three (3) of the credit/debit cards used to pay this Nextiva account are 4250-3200-2513-0643 (Green Dot Bank - Prepaid Visa), 4000-5403-0169-7568 (Meta Bank - Prepaid Visa), and 4000-5403-0162-1196 (Meta Bank - Prepaid Visa).

13. Subpoenaed records from Green Dot Bank and Meta Bank related to these three (3) financial accounts revealed that the account holder for each account is ANNE EASON, (dob: 2-15-1947), SSN 420-66-8423, 1510 Indian Pass Rd. Port Saint Joe, FL 32456, with a listed email account of **annebeason47@gmail.com**. Searches of law enforcement databases reveal that a person named ANNE EASON with the same date of birth, social security number, and address does in fact exist. Subpoenaed records from Google, Inc. related to email address **annebeason47@gmail.com** revealed that the phone number provided for this email address is (810) 487-4511, which is one of the Nextiva phone numbers associated with GOLDPHARMA24's customer service phone number, and the listed recovery email address for the **annebeason47@gmail.com** email address is **jessicagilmore24hs@gmail.com**.

14. On June 25, 2015, case agents conducted an undercover purchase from the GOLDPHARMA24 internet pharmacy at website [www.goldpharma-24.com](http://www.goldpharma-24.com). Case agents attempted to purchase 60 tablets of Percocet 10mg (oxycodone, a schedule II controlled substance). To facilitate the purchase, case agents were instructed to wire money by Western Union to MOHD SABUDDIN RAFIK SHAIKH in India. Case agents subsequently received a shipment from India of red tablets which were not the ordered Percocet.

15. After receiving the red tablets instead of the ordered Percocets, case agents contacted the GOLDPHARMA24 website via telephone and emails in response to not receiving the ordered product. Case agents were informed that they did not have a distributor who could reship Percocet at this time so case agents were instructed to select anything else off their internet pharmacy website to order. Case agents subsequently ordered and received in September 2015 90 tablets of Tramadol 200mg (a schedule IV controlled substance) from India and 60 tablets of Xanax .25mg (alprazolam, a schedule IV controlled substance) from Romania. These medications were sent to the DEA laboratory in Chicago and tested positive for the presence of the indicated drugs. Along with the Xanax medication, case agents received a computer printed and electronically signed prescription in the undercover name by Dr. LADISLAV SMRCEK. The undercover agent never received an examination and was never questioned about medical history, current medications, or symptoms which would be required to be prescribed this medication.

16. Case agents communicated with GOLDPHARMA24 representatives at customer service telephone number 810-487-4516 and received emails regarding the undercover purchase from email address **ameliagrey24hs@gmail.com**. Case agents determined that for many of the communications via email, the GOLDPHARMA24 representative was utilizing IP addresses 107.170.93.126 or 209.160.64.134, which is owned by Internet Service Provider (ISP) Digital Ocean. Subpoenaed records from Digital Ocean revealed that IP address 107.170.93.126 is one of several IP addresses assigned to servers rented by the same customer and many of the server names are related to prescription medications. This account has been paid by PayPal accounts in the name of JIMMY LE with an email address of **jimmy\_le5252@yahoo.com** and RAMONA ENRIQUETA IBARRA with an email address of **ramonaenibarra@gmail.com**.

17. Case agents determined that IP address 209.160.64.134 is owned by ISP HopOne Internet Corporation. Subpoenaed records from HopOne Internet Corporation revealed that this IP address 209.160.64.134 is listed to RAMONA ENRIQUETA IBARRA, 245 Montaneses, Barrio Libertad, Buenos Aires, 1718 Argentina. Case agents contacted DEA Special Agent Brandon Moles who is assigned to the DEA Buenos Aires, Argentina Office. Special Agent Moles checked the address 245 Montaneses, Barrio Libertad, Buenos Aires 1718 Argentina and confirmed that this address does exist and the residents residing there have the last name of IBARRA.

18. Subpoenaed records from Western Union revealed that there was another potential customer of GOLDPHARMA24 who also wired money to MOHD SABUDDIN

RAFIK SHAIKH in India. This potential customer was identified as JAMES E. CARTER residing in Brooklyn Park, Minnesota. Subpoenaed records revealed that CARTER wired money at least fourteen (14) times to people in India, Romania, and Pakistan. In August of 2015, case agents interviewed CARTER. CARTER stated that he first located an internet pharmacy located at [www.24hsmeds.com](http://www.24hsmeds.com) and he stated he has purchased Tramadol (schedule IV controlled substance) from this internet pharmacy numerous times without a prescription. CARTER showed case agents the emails he received related to these orders, which revealed that he communicated by email with [jessicagilmore24hs@gmail.com](mailto:jessicagilmore24hs@gmail.com) and [pennysenn24hs@gmail.com](mailto:pennysenn24hs@gmail.com) regarding his purchases of controlled substances. CARTER also stated that he communicated by telephone with the representative at 810-487-4516, which is the same telephone number used by GOLDPHARMA24. CARTER voluntarily turned over to case agents a quantity of Tramadol and suspected Viagra pills, which he said he purchased from the internet pharmacy.

19. On August 28, 2015, case agents conducted an undercover purchase from the GOLDPHARMA24 internet pharmacy at website [www.goldpharma-24.com](http://www.goldpharma-24.com). Case agents purchased 180 tablets of Soma 500mg (carisoprodol, which is a schedule IV controlled substance) and 120 tablets of Valium (diazepam, which is a schedule IV controlled substance). In connection with the purchase, case agents were instructed via [ameliagrey24hs@gmail.com](mailto:ameliagrey24hs@gmail.com) to wire money by Western Union to CHARANJEET KAUR in India. Case agents received a shipment from India of the 180 tablets of Soma 500mg and a shipment from Romania of the 120 tablets of Valium accompanied by another

computer printed prescription with an electronic signature of Dr. LADISLAV SMRCEK. The Soma 500mg tablets were sent to the DEA laboratory in Chicago and did test positive for the presence of the indicated drug. Subpoenaed records from Western Union revealed there were another nine (9) potential customers who also wired money to CHARANJEET KAUR in India.

20. Subpoenaed records from PayPal for the active account affiliated with email address [ramonaenibarra@gmail.com](mailto:ramonaenibarra@gmail.com) reveal the account holder to be: RAMONA ENRIQUETA IBARRA, (dob: 07-18-1960), 245 Montaneses Barrio Libertad, Buenos Aires 1718, Argentina. The records reveal that the RAMONA IBARRA PayPal account was logged into using the HopOne IP address listing to customer RAMONA ENRIQUETA IBARRA and the PayPal account records reveal payments made to ISP Digital Ocean, payments made to numerous server and domain companies, and money being transferred back and forth between this RAMONA IBARRA PayPal account and PayPal account assigned email address [jimmy\\_le5252@yahoo.com](mailto:jimmy_le5252@yahoo.com).

21. Subpoenaed records from PayPal for the active account affiliated with email address [jimmy\\_le5252@yahoo.com](mailto:jimmy_le5252@yahoo.com) reveal the account holder to be JIMMY LE, (dob: 10-27-1981), SSN: 573-67-1200, 2602 S. Poplar St. Santa Ana, California 92704. Searches of law enforcement databases reveal that a person named JIMMY LE with the same date of birth, social security number, and address does in fact exist. The PayPal records also reveal another person added to the account: RAMONA IBARRA, 1510 Indian Pass Road Port Saint Joe, Florida 32456, which is the same address of ANNE EASON with email address [annebeason47@gmail.com](mailto:annebeason47@gmail.com).

22. This JIMMY LE PayPal account was logged into 1,611 times using HopOne IP address listing to customer RAMONA ENRIQUETA IBARRA. Case agents reviewed transactions from this PayPal account and observed payments made to ISP Digital Ocean, payments made to numerous server and domain companies, and money being transferred back and forth between this JIMMY LE PayPal account and PayPal account assigned email address **ramonaenibarra@gmail.com**. The PayPal records also revealed transactions with ANNE EASON and payments received from the same people repeatedly, which case agents believe are customers purchasing prescription drug refills. One of these potential customers is BEVERLY E. BOOTZEN who resides in Mequon, Wisconsin.

23. In January of 2016, case agents interviewed BEVERLY E. BOOTZEN, who had been making payments to the JIMMY LE PayPal account. BOOTZEN stated she has purchased controlled substances from internet pharmacies without a prescription. She recalled specifically purchasing Tramadol (a schedule IV controlled substance) multiple times and the past few times she was directed to make payment by PayPal into the JIMMY LE PayPal account with email address **jimmy\_le5252@yahoo.com**. BOOTZEN could not recall the specific internet pharmacy names she purchased from, but did provide a pharmacy representative email address she communicated with of **jessicagilmore24hs@gmail.com** and phone numbers of (810) 487-4510 and (810) 487-4511, both of which are telephone numbers associated with the GOLDPHARMA24 Nextiva phone account. BOOTZEN voluntarily turned over to case agents a quantity of

tablets represented to be Tramadol that she purchased by sending money to the JIMMY LE PayPal account,

24. On February 2, 2016, case agents executed a federal search warrant at the residence of ANTHONY T. HARDY located at 1511 Brady Ct. Bowie, Maryland 20721. HARDY agreed to cooperate and voluntarily provided a statement to law enforcement. HARDY admitted to being involved in internet pharmacies since approximately 1999 or 2000. HARDY stated he is a member of multiple affiliate groups that sell controlled and non-controlled prescription medications. HARDY stated that his role was to register thousands of prescription drug domains and create websites for the affiliate groups. HARDY stated that he would then be paid a commission based on how many customers would purchase prescription drugs from his domains or through his links directing the customers to the affiliate group's websites. HARDY would pay internet-based companies to help promote and advertise his websites and links. HARDY stated that he had no role in taking the drug orders or shipping the drugs as that role is handled by other unknown persons in the organization.

25. HARDY identified the affiliate group which sold the majority of controlled substances as the "Biff Affiliate Group." HARDY gave consent for investigators to log into this account using his username and password. It was confirmed that GOLDPHARMA24 is an internet pharmacy affiliated with this "Biff Affiliate Group." HARDY stated that the affiliate group manager who he communicated with about business and payments is "Biff Tannen" with email address 01biftannen@gmail.com. This contact information for the affiliate manager was



accessible by investigators only after logging into HARDY's account as an affiliate group member. HARDY stated that he believed he was paid commission by this affiliate group into his PayPal account. Case agents then executed a search warrant on Comcast Internet Provider and received email content related to HARDY's athardy@comcast.net email account. Case agents reviewed these emails and found email communication between HARDY and "Biff Tannen" regarding GOLDPHARMA24, including emails in which HARDY was requesting his commission. HARDY was communicating with "Biff Tannen" at **bifftannen01@yahoo.com.ar**.

26. Based on my training and experience, individuals who engage in interstate trafficking in controlled and non-controlled pharmaceuticals via the internet will communicate and send and receive information through electronic communication such as e-mails. Individuals engaged in criminal activity via the internet often remain anonymous by providing inaccurate or false information, but will often use e-mail accounts to conduct business and or communicate with other co-conspirators. The true identity and location of these individuals can often be found by analyzing their e-mail communication.

27. In general, an e-mail that is sent to a Google or Yahoo subscriber is stored in the subscriber's "mail box" on Google and Yahoo's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google and Yahoo's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google or Yahoo's servers for a certain period of time.

### BACKGROUND CONCERNING E-MAIL

28. In my training and experience, I have learned that Google and Yahoo provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google and Yahoo allow subscribers to obtain e-mail accounts at the domain name yahoo.com and gmail.com. Subscribers obtain an account by registering with Google or Yahoo. During the registration process, Google and Yahoo ask subscribers to provide basic personal information. Therefore, the computers of Google and Yahoo are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google and Yahoo subscribers) and information concerning subscribers and their use of Google or Yahoo's services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

31. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

### CONCLUSION

32. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrant will be served on Google and Yahoo who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

## ATTACHMENT A

### **Property to Be Searched**

This warrant applies to information associated with the following six email addresses that are stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain View, California.

1. 01bifftannen@gmail.com
2. jessicagilmore24hs@gmail.com
3. ramonaenibarra@gmail.com
4. annebeason47@gmail.com
5. ameliagrey24hs@gmail.com
6. pennysenn24hs@gmail.com

## ATTACHMENT B

### Particular Things to be Seized

#### I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.



## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code, Sections 829(e), 841(a)(1), 841(h), and 843(c)(2)(A) and occurring after January 1, 2015, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The importation and distribution of controlled substances and other prescription medications.
- b. Information relating to the identity of any and all individuals who operate or maintain online pharmacies that sell controlled substances and other prescription medications.
- c. Records of payment made in relation to the operation and maintenance of online pharmacies that sell controlled substances and other prescription medications, including proceeds from such sales.
- d. Information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.